AMENDMENTS TO THE SPECIFICATION

Please delete Paragraphs [0037] through [0052] of the specification.

Please add the following paragraphs.

[0052.1] The embodiment of the present invention provides a digital certificate issuing system with intrusion tolerance ability, the system includes: an offline secret key distributor, at least one online task distributor, k online secret share calculators and m online secret share combiners;

the offline secret key distributor is configured for splitting a private key into multiple first sub-secret-keys d_{ji} and multiple second sub-secret-keys, sending the first sub-secret-keys d_{ji} to the k online secret share calculators; sending the second sub-secret-keys and equation combination representations corresponding to the second sub-secret-keys to the m online secret share combiners; and the private key is constructed by one second sub-secret-key and t first sub-secret-keys d_{ji}, each equation combination representation comprises t items of j and i, j is sequence number of the secret share calculator and i is number of the first sub-secret-key in the j^{th} secret share calculator, and each of j in one equation combination representation is different;

the at least one online task distributor is configured for sending out a certificate to be signed through a first broadcast channel;

the k online secret share calculators are configured for checking correctness of the certificate to be signed, calculating at least t first calculation results according to first sub-secret-keys stored and the certificate to be signed, and sending out the at least t

first calculation results, at least t items of j and i corresponding to the at least t first calculation results respectively through a second broadcast channel; and

the m online secret share combiners are configured for matching t items of j and i received through the second broadcast channel with the equation combination representations stored, and determining a matched online secret combiner storing the matched equation combination representation including t items of j and i;

the matched online secret share combiner is configured for checking the correctness of the certificate to be signed, calculating a second calculation result according to the certificate to be signed and the second sub-secret-key corresponding to the matched equation combination representation, calculating a digital signature according to the t first calculation results corresponding to the t items of i and j in the matched equation combination representation and the second calculation result, generating a digital certificate according to the digital signature and contents of the certificate to be signed;

j, i, k, t and m are positive integers, and t is less than k.

[0052.2] The embodiment of the present invention also provides a method for a digital certificate issuing system with intrusion tolerance ability issuing digital certificate, the method includes:

splitting a private key into multiple first sub-secret-keys and multiple second sub-secret-keys, wherein the private key is constructed by one second sub-secret-key and t first sub-secret-keys, the second sub-secret-key corresponds to the t first sub-secret-

keys according to an equation combination representation, and the number t is a positive integer;

calculating t first calculation results according to the certificate to be signed and the t first sub-secret-keys in the multiple first sub-secret-keys upon receiving a certificate to be signed;

obtaining the second sub-secret-key corresponding to the t first sub-secret-keys according to the equation combination representation;

calculating a second calculation result according to the second sub-secret-key obtained and the certificate to be signed;

generating a digital signature according to the t first calculation results and the second calculation result;

generating a digital certificate according to the digital signature and contents of the certificate to be signed.

Please replace Paragraph [0054] with the following paragraph rewritten in amendment format:

[0054] The method and system according to the invention have the following characteristics:

1. The online task distributor can broadcast a digital signature task without selecting secret share calculators and specifying sub-secret-keys, so when system is updating, the online task distributor will not be affected, and when a secret share

calculator is damaged suddenly, execution time for broadcasting a task will not be affected too.

2. When adding a secret share calculator, it is necessary only to generate a set of first sub-secret-keys for the new secret share calculator. The offline secret-key distributor can make equation combination according to the number of the newly added secret share calculator and the numbers of existing secret share calculators, compute the corresponding second sub-secret-key ~~ca~~c_a, and then add the new equation combination representation and ~~ca~~ c_a to the secret share combiner in a way accepted by administration. The adding will not affect the system normal operation.

3. When taking away a secret share calculator, shutting down the device is enough; for efficiency reason, equation combination representation including the secret share calculator number and corresponding ~~ca~~ c_a can be deleted.

4. The invention has the intrusion tolerance ability as other schemes mentioned in background section. When less than t secret share calculators are intruded, the system secret key d will not be leaked. Since secret share combiners are added, even all secret share calculators are intruded, the system secret key d will not be leaked also. It can be proved theoretically that attacking secret share combiners cannot obtain the system secret key d; although there are many equations, the rank of coefficient matrix of the equations is less than the number of variables.

5. The invention can resist a conspiracy attack from the secret share calculator and the secret share combiner, i.e. even when a conspiracy attack is done by a secret share calculator and a secret share combiners, the system secret key d will not

be leaked, furthermore, comparing with other schemes, the number of the secret share combiners can be less greatly, for example, when k = 5 and t = 3, the least number of secret share combiners is 2.

6. An operator confirmation is added during distributing private key and issuing certificate, which will further guarantee security and reliability of issuing digital certificate. Further areas of applicability of the present invention will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating the preferred embodiment of the invention, are intended for purposes of illustration only and are not intended to limit the scope of the invention.

Please replace Paragraph [0064] with the following paragraph rewritten in amendment format:

[0064] The processing of sharing secret d in this system structure is completed through two layers of components: one layer of components ~~are~~ is composed of secret share calculators 23 and another layer of components are composed of secret share combiners 24. More than one d_{ji} are respectively stored in the secret share calculators 23, and c_a is stored in the secret share combiners 24. In this way, a two-layer secret share structure is formed. Two layers of components respectively store first sub-secret-key d_{ji} and second sub-secret-key c_a. The first sub-secret-key d_{ji} employs two digits as its suffix, among them the first digit j is a sequence

number, i.e. device number, of the secret share calculators 23, j = 1, 2 ... k, and the second digit i is a number of the secret keys stored in a certain secret share calculator 23, i = 1, 2 ... l. For example, when a secret share calculator 23 stores two items of d_{ji}, the first sub-secret-key respectively are d_{j1} and d_{j2}, meanwhile d_{11} and d_{12} represent two items of first sub-secret-keys stored in the first secret share calculator. The a is the second sub-secret-key number inside the machine of the secret share combiner.